

Of the rejected claims, only claims 1, 9, and 12 are independent. This response, at least initially, focuses on these independent claims.

First, independent claim 1, among a number of unique features, recites: “wherein said user device is a user key or a lock of a master key system...in case said authentication process was successful, carrying out a software operation by said first system device, by which software operation said encryption key stored in said first user device is replaced by a second encryption key, wherein said second encryption key is stored in second system devices and further user devices used in a second level of said key and lock system, thereby making said user device operable with said second system and further user devices.” The Examiner alleges that claim 1 is directed to a method of authorizing a user device of a key and lock system and is anticipated by the teachings of Uemura. Applicant respectfully disagrees. Applicant has carefully studied Uemura’s discussion of the card issuing machine issuing guest cards, which is not similar to having a user device such as a key or a lock in which a first encryption key is replaced with a second encryption key making this user device operable with the devices of the second system and further user devices as set forth in claim 1.

Uemura, on the other hand, discloses a method of issuing cards by using a card issuing machine including a memory having stored therein an initial secret code, a card reader, and a keyboard. In Uemura, this initial secret code is keyed in and upon a match, a new secret code is keyed in for associating a first card with the card issuing machine (*see* Abstract). That is, Uemura has nothing to do with a master key system as set forth in claim 1. A master key system enables various persons with different access authorization to open all relevant doors with only

one key.¹ Uemura simply relates to a method and a system for issuing cards in a hotel but is unrelated to a master key system, as set forth in claim 1. In short, Uemura addresses an unrelated problem and fails to teach or suggest a master key system set forth in claim 1.

More particularly, Uemura teaches the first card being issued by the card issuing machine on condition that the secret code keyed-in matches the initial secret code stored in the memory of the machine. At this time, a code for associating the first card with the card issuing machine is keyed in and stored in the first card and in the machine. With the issue of the first card, the first card is closely associated with the issuing machine. The first card is of the highest level and serves as a key for issuing another card of lower level (col. 3, lines 10 to 44).

The Examiner appears to equate a card issuing machine of Uemura with a user device, as set forth in claim 1 (*see* pages 2 and 6 of the Office Action). Applicant respectfully submits, however, that a card issuing machine is neither a user key nor a user lock. Moreover, the card issuing machine is not part of a master key system. Furthermore, Applicant respectfully submits that one of ordinary skill in the art would have understood that a user device is used by the end user such as a key and that a system device are devices used by other personnel such as locksmiths and service personnel. Accordingly, Uemura's card issuing machine cannot be equated to a user device and Uemura's cards such as guest cards are not system devices but, on the contrary, user devices. In short, Applicant respectfully submits that Uemura's card issuing machine is not a user machine within the meaning of claim 1, *i.e.*, a user key or a lock as set forth in claim 1.

¹ <http://www.evva.com/SchlieszanlageE.htm>, accessed August 31, 2005, a copy is provided.

Moreover, Uemura only discloses that a secret code is associated with a respective card. That is, in Uemura, the first secret code is associated with the first card and the second secret code is associated with the second card (col. 3, lines 19 to 33). Accordingly, Uemura fails to teach or suggest having a first encryption code be replaced with the second encryption key in that same user device. In Uemura, the guest cards are blank before they are programmed by the card issuing machine (col. 17, line 52 to col. 18, line 4). Accordingly, Uemura does not teach or suggest replacing one code with another code in the same device. That is, Uemura is not directed to a distribution of keys and locks and a key device, which is difficult to copy without knowledge of the system. In other words, Uemura does not address the problem of secure distribution of keys and locks. In short, each card of Uemura is associated with its own respective secret code and there is no teaching or suggestion of replacing a secret code with another secret code.

Further, in Uemura, the secret codes are used in communication with the card issuing machine and not with the second system of devices and further user devices. That is, Uemura fails to teach or suggest having the second secret code be present in all second level devices to be used during the authentication process between these devices. In Uemura, the secret code (alleged encryption key) is only used in communication between a card and a card issuing machine and not in authentication of all second level devices such as a second system of devices and further user devices.

Therefore, “wherein said user device is a user key or a lock of a master key system...in case said authentication process was successful, carrying out a software operation by said first

RESPONSE UNDER 37 C.F.R. § 1.116
U.S. Appln. No. 09/802,931
Attorney Docket No.: Q63553

system device, by which software operation said encryption key stored in said first user device is replaced by a second encryption key, wherein said second encryption key is stored in second system devices and further user devices used in a second level of said key and lock system, thereby making said user device operable with said second system and further user devices,” as set forth in claim 1 is not taught or suggested by Uemura, which lacks having one encryption key be replaced by another encryption key in the same user device and which lacks having the user device use the second encryption key with system devices of the second level and further user devices. For at least these exemplary reasons, claim 1 distinguishes from Uemura. Therefore, Applicant respectfully requests the Examiner to withdraw this rejection of claim 1. Claims 2-8 are patentable at least by virtue of their dependency on claim 1.

In addition, dependent claim 8 recites: “wherein said electronic encryption keys are unreadable from outside said electronic circuitry.” The Examiner alleges that when a guest card is invalid, it is equivalent to the card being unreadable from the outside (*see* page 5 of the Office Action). Applicant respectfully disagrees. It is respectfully submitted that in Uemura, the secret code is stored on a magnetic strip, which is read by the card issuing machine. It is thus clear that this information is readable from outside of the card. That is, information on the card is read to indicate that overtime has occurred so as to output “invalid” (col. 29, lines 40-47). However, having the card being read to output invalid is not equivalent and cannot be compared to a code unreadable from the outside. For at least this additional reason, Applicant respectfully submits that claim 8 patentably distinguishes from Uemura.

RESPONSE UNDER 37 C.F.R. § 1.116
U.S. Appln. No. 09/802,931
Attorney Docket No.: Q63553

Claims 9 and 12 recite features similar to the features argued above with respect to claim 1. Therefore, arguments presented with respect to claim 1 are respectfully submitted to apply with equal force here. Applicant therefore respectfully requests the Examiner to withdraw this rejection of independent claims 9 and 12. Also, Applicant respectfully submits that claims 10 and 11 are allowable at least by virtue of their dependency on claim 9.

Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly invited to contact the undersigned attorney at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

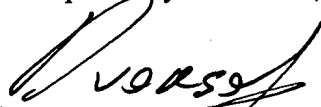
WASHINGTON OFFICE

23373

CUSTOMER NUMBER

Date: September 2, 2005

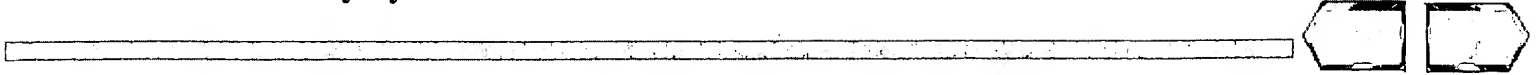
Respectfully submitted,



Nataliya Dyorson
Registration No. 56,616

Attorney Docket No.: Q63553

What is a "Master Key System"?



A master key system enables various persons with different access authorizations to open all relevant doors with only one key.

Your advantages:

- ✓ Security with only a few keys.
- ✓ Comfort, since there is only one key for all relevant doors.
- ✓ Organization is simplified.
- ✓ You can exactly determine, which persons have access for which rooms.
- ✓ All cylinder locks and types (main entrance, internal doors, garage doors, ...) can be opened with one key.

Example:

Grand Master Key System for an office building used by two companies.

GMK: General Master Key opens all doors (e.g. for security guard).

MK 1: Master Key 1 opens all doors for Messrs. Smith (e.g. for Director Smith).

1SMK 1: Submaster Key 1 opens the main entrance and all adjoining rooms (lavatory, kitchen, store room, ...)

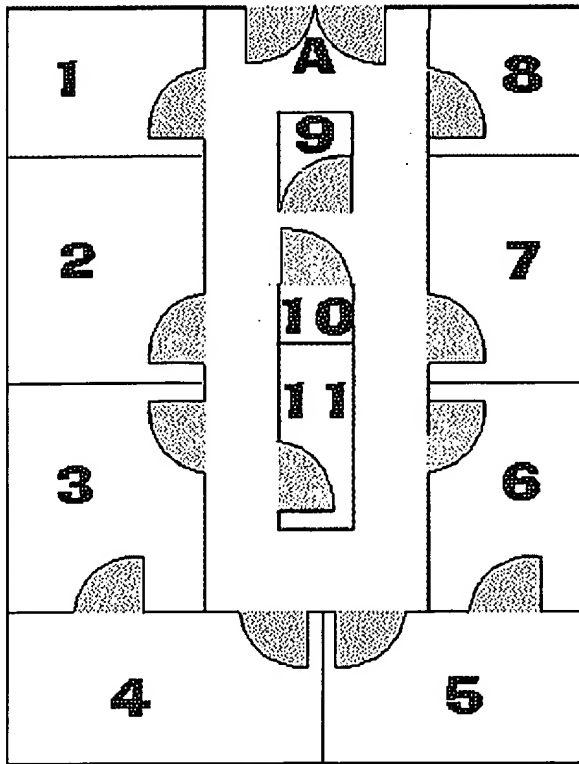
1SMK 2: Submaster Key 2 opens main entrance, adjoining rooms and all secretary doors (e.g. key for secretary of director Smith).

MK 2: Master Key 2 opens all doors for Messrs. Berger.

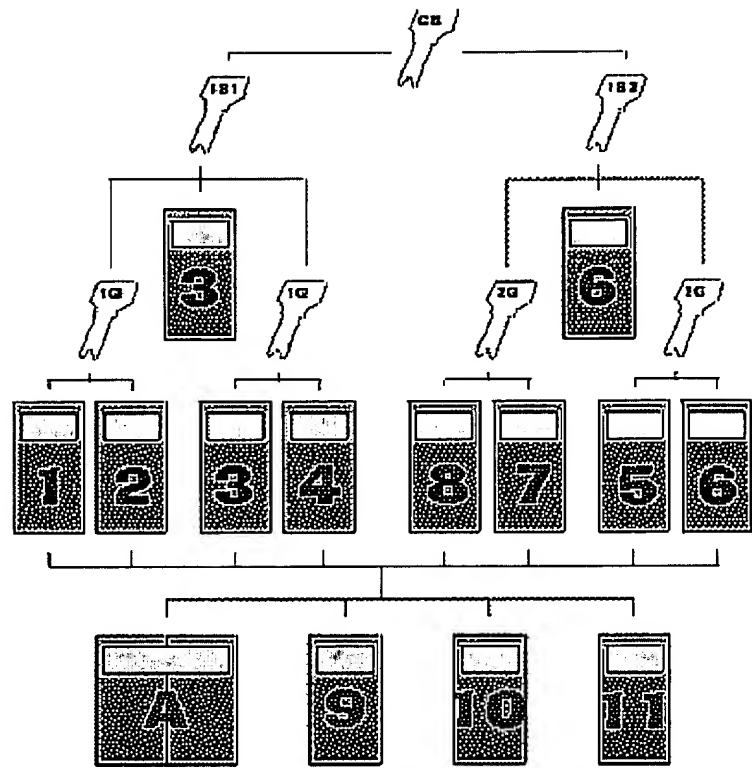
2SMK 1: This submaster opens only the doors of the purchasing and sales area, the main entrance and adjoining doors (e.g. key for all commercial clerks).

2SMK 2: This submaster opens main entrance, adjoining rooms and secretary doors (key for secretary of Messrs. Berger).

Graphic Description:



- | | |
|------------------------|------------------------------|
| 1...Office 1 Smith | 2...Office 2 Smith |
| 5...Secretariat Berger | 6...Director's Office Berger |
| 9...Store room | 10...Lavatory |



- | | |
|-----------------------------|-----------------------|
| 3...Director's Office Smith | 4...Secretariat Smith |
| 7...Purchase Berger | 8...Sales Berger |
| 11...Kitchen | A...Main Entrance |

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.